UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/086,107	02/28/2002	John Paul Lachman III	08475.105003	2755

7590 09/27/2006

RICHARD CUSICK, ESQ.
CYBER OPERATIONS, LLC.
ATTN: LEGAL DEPARTMENT
153 CHABA VALLEY PARKWAY
PELHAM, AL 35124

EXAMINER	
REZA, MOHAMMAD W	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 09/27/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/086,107	LACHMAN ET AL.	
	Examiner	Art Unit	
	Mohammad W. Reza	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 February 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-70* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-70* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *09/21/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-70 are presented for examination

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:
Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 1, 15, 27, 30, 33, and 42 are rejected under 35 U.S.C. 101 because the claim invention is directed to non-statutory subject matter. According to the specification of the invention (The present invention also includes a computer program which embodies the functions described herein and illustrated in the appended flow charts. However, it should be apparent that there could be many different ways of implementing the invention in computer programming, and the invention should not be construed as limited to any one set of computer program instructions. Further, a skilled programmer would be able to write such a computer program to implement the disclosed invention based on the flow charts and associated description in the application text, for example. Therefore, disclosure of a particular set of program code instructions is not considered necessary for an adequate understanding of how to make and use the invention, paragraphs, 0064) a computer program (computer implemented method) is reasonably interpreted by one of ordinary skill as just software, it is a system of software, per se. In these claims the function of the program is just software not any hardware. Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760 (claim to a data structure per se held nonstatutory). Data structures not claimed as embodied in computer-readable media are descriptive material per se and are not statutory because they are

not capable of causing functional change in the computer. Such claimed data structures do not define any structural and functional interrelationships between the data structure and other claimed aspects of the invention which permit the data structure's functionality to be realized. Similarly, computer programs claimed as computer instructions per se, i.e., the descriptions or expressions of the programs, are not physical "things." They are neither computer components nor statutory processes, as they are not "acts" being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed elements of a computer which permit the computer program's functionality to be realized. Accordingly, it is important to distinguish claims that define descriptive material per se from claims that define statutory inventions. So, it does not appear that a claim reciting software with functional descriptive material falls within any of the categories of patentable subject matter set forth in § 101.

3. Claims 14, 26, 29, 32, 41, 51 are rejected under 35 U.S.C. 101 because the claim invention is directed to non-statutory subject matter. According to the specification of the invention (Page 1-53) a computer readable medium program is reasonably interpreted by one of ordinary skill as just software, it is a system of software, per se. In this claim the function of the program is just software not any hardware. Warmerdam, 33 F.3d at 1360-61, 31 USPQ2d at 1759 (claim to computer having a specific data structure stored in memory held statutory product-by-process claim) with Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760 (claim to a data structure per se held nonstatutory). See, e.g., Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760 (claim to a

data structure per se held nonstatutory). Such claimed data structures do not define any structural and functional interrelationships between the data structure and other claimed aspects of the invention which permit the data structure's functionality to be realized. In contrast, a claimed computer program encoded with a data structure defines structural and functional interrelationships between the data structure and the computer software and hardware components which permit the data structure's functionality to be realized, and is thus statutory. Similarly, computer programs claimed as computer instructions per se, i.e., the descriptions or expressions of the programs, are not physical "things." They are neither computer components nor statutory processes, as they are not "acts" being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed elements of a computer which permit the computer program's functionality to be realized. Accordingly, it is important to distinguish claims that define descriptive material per se from claims that define statutory inventions. So, it does not appear that a claim reciting software with functional descriptive material falls within any of the categories of patentable subject matter set forth in § 101.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an

international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-70 are rejected under 35 U.S.C. 102(e) as being anticipated by Maher, III et al hereafter Maher (US patent 6910134).

5. As per claim 1, and 14, Maher discloses a computer-implemented method comprising the steps of: passively collecting a data packet from data received by the host network, the data packet comprising information indicating the attack (col. 4, lines 43-67, col. 7, lines 10-18); comparing the information in the data packet to a signature of an attack type of the attack to determine whether the information and the signature comprise matching data; and detecting the attack in response to a determination that the signature and the information comprise matching data (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 10, lines 19-42).

6. As per claim 2, Maher discloses the method comprising the step of providing a pathway for an offensive countermeasure against a source of the attack (col. 3, lines 60-67, col. 4, lines 1-26, col. 6, lines 19-36).

7. As per claim 3, Maher discloses the method comprising the step of generating the signature for the attack type of the attack (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 10, lines 19-42).

8. As per claim 4, Maher discloses the method wherein the attack type comprises a plurality of data packets, and wherein said generating step comprises the steps of: identifying a repetitive pattern in the plurality of data packets of the attack type; and storing the repetitive pattern as the signature of the attack type (col. 1, lines 45-67, col.

2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 8, lines 27-64, col. 10, lines 19-42).

9. As per claim 5, Maher discloses the method wherein the information comprises information from a header of the data packet, and wherein said comparing step comprises comparing the information from the header to the signature (col. 4, lines 43-67, col. 5, lines 58-67).

10. As per claim 6, Maher discloses the method wherein the signature comprises a repetitive pattern of information from data packets of the attack type (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 8, lines 27-64, col. 10, lines 19-42).

11. As per claim 7, Maher discloses the method wherein the repetitive pattern comprises information included in a header of each data packet of the attack type (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 8, lines 27-64, col. 10, lines 19-42, col. 4, lines 43-67, col. 5, lines 58-67).

12. As per claim 8-9, Maher discloses the method comprising the step of initiating a defensive countermeasure to protect the host network from the attack in response to detection of the attack, and comprising the step of confirming the attack before initiating the defensive countermeasure to protect the host network from the attack (col. 4, lines 43-67, col. 7, lines 10-18, col. 3, lines 60-67, col. 4, lines 1-26, col. 6, lines 19-36).

13. As per claim 10, Maher discloses the method wherein said confirming step comprises the steps of: setting a load threshold for the host network; determining the current load on the host network; determining whether the current load exceeds the load

threshold; and confirming the attack in response to a determination that the current load exceeds the load threshold (col. 4, lines 43-67, col. 7, lines 10-18, col. 3, lines 60-67, col. 4, lines 1-26, col. 6, lines 19-36).

14. As per claim 11, Maher discloses the method comprising the step of tracing a route of the attack to determine whether a single source produced the attack, wherein said initiating step comprises initiating a single-source, defensive countermeasure in response to a determination that a single source produced the attack, and wherein said initiating step comprises initiating a multiple-source, defensive countermeasure in response to a determination that a single source did not produce the attack (col. 3, lines 61-67, col. 4, lines 1-26, col. 5, lines 5-22, col. 6, lines 19-36).

15. As per claim 12, Maher discloses the method wherein said collecting step comprises collecting a plurality of data packets from data received by the host network, wherein said tracing step comprises comparing information in each of the data packets to determine if the information in each data packet is the same, and wherein said tracing step determines that a single source produced the attack in response to a determination that the information in each data packet is the same (col. 3, lines 61-67, col. 4, lines 1-26, col. 5, lines 5-22, col. 6, lines 19-36, col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 10, lines 19-42).

16. As per claim 13, Maher discloses the method wherein the information in each data packet comprises a source IP address (col. 3, lines 61-67, col. 4, lines 1-26, col. 5, lines 5-22, col. 6, lines 19-36).

17. As per claim 15, and 26, Maher discloses a computer-implemented method comprising the steps of: passively collecting a plurality of data packets from data received by the host network (col. 4, lines 43-67, col. 7, lines 10-18); comparing information in respective data packets to determine if any pair of the data packets comprise similar information; and detecting the attack in response to a determination that the pair of data packets comprise similar information (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 10, lines 19-42).

18. As per claim 16, Maher discloses the method comprising the step of providing a pathway for an offensive countermeasure against a source of the attack (col. 3, lines 60-67, col. 4, lines 1-26, col. 6, lines 19-36).

19. As per claim 17, Maher discloses the method wherein said comparing step comprises comparing information in the respective data packets to determine if about forty percent of the data packets comprise similar information, and wherein said detecting step detects the attack in response to a determination that about forty percent of the data packets comprise similar information (col. 4, lines 43-67, col. 7, lines 10-18).

20. As per claim 18, Maher discloses the method wherein the information in the respective data packets comprises a header, and wherein said comparing step comprises comparing the headers of the respective data packets (col. 4, lines 43-67, col. 5, lines 58-67).

21. As per claim 19, Maher discloses the method comprising the steps of: setting a load threshold for the host network; determining the current load on the host network; comparing the current load to the load threshold; and confirming the attack when the

current load exceeds the load threshold (col. 4, lines 43-67, col. 7, lines 10-18, col. 3, lines 60-67, col. 4, lines 1-26, col. 6, lines 19-36).

22. As per claim 20, Maher discloses the method comprising the steps of: determining whether the attack comprises a new attack type; and learning a new signature of the new attack type in response to a determination that the attack comprises a new attack type (col. 6, lines 58-67, col. 7, lines 1-9).

23. As per claim 21, Maher discloses the method wherein said learning step comprises the steps of: identifying a repetitive pattern in data from the plurality of data packets of the attack; and storing the repetitive pattern as the new signature of the new attack type (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 8, lines 27-64, col. 10, lines 19-42).

24. As per claim 22, Maher discloses the method wherein the data from the plurality of data packets comprises a header for each respective data packet, and wherein said identifying step comprises identifying a repetitive pattern in the headers of the plurality of data packets of the new attack type (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 8, lines 27-64, col. 10, lines 19-42, col. 6, lines 58-67, col. 7, lines 1-9).

25. As per claim 23, Maher discloses the method comprising the step of initiating a defensive countermeasure to protect the host network from the attack in response to detection of the attack (col. 3, lines 60-67, col. 4, lines 1-26, col. 6, lines 19-36).

26. As per claim 24, Maher discloses the method comprising the step of tracing a route of the attack to determine whether a single source produced the attack, wherein

said initiating step comprises initiating a single-source, defensive countermeasure in response to a determination that a single source produced the attack, and wherein said initiating step comprises initiating a multiple-source, defensive countermeasure in response to a determination that a single source did not produce the attack (col. 3, lines 61-67, col. 4, lines 1-26, col. 5, lines 5-22, col. 6, lines 19-36).

27. As per claim 25, Maher discloses the method wherein said tracing step comprises comparing a source IP address in each of the data packets to determine if the source IP address in each data packet is the same, and wherein said tracing step determines that a single source produced the attack in response to a determination that the information in each data packet is the same (col. 3, lines 61-67, col. 4, lines 1-26, col. 5, lines 5-22, col. 6, lines 19-36).

28. As per claim 27, and 29 Maher discloses a computer-implemented method comprising the steps of: detecting the attack based on a load capacity of the host network (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 10, lines 19-42); and initiating a defensive countermeasure to protect the host network from the attack in response to detection of the attack (col. 3, lines 60-67, col. 4, lines 1-26, col. 6, lines 19-36).

29. As per claim 28, Maher discloses the method wherein said detecting step comprises the steps of: setting a load threshold for the host network, the load threshold establishing an amount of the load capacity beyond which the attack is indicated; determining the current load on the host network; and comparing the current load to the load threshold, wherein said detecting step detects the attack when the current load

exceeds the load threshold (col. 4, lines 43-67, col. 7, lines 10-18, col. 3, lines 60-67, col. 4, lines 1-26, col. 6, lines 19-36).

30. As per claim 30, and 32 Maher discloses a computer-implemented method comprising the steps of: examining information included in each of the plurality of data packets (col. 4, lines 43-67, col. 7, lines 10-18); identifying a repetitive pattern in the information of at least two of the plurality of data packets; and storing the repetitive pattern as a signature of the attack type (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 10, lines 19-42, col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 8, lines 27-64, col. 10, lines 19-42).

31. As per claim 31, Maher discloses the method wherein the information comprises a header (col. 4, lines 43-67, col. 5, lines 58-67).

32. As per claim 33, and 41 Maher discloses a computer-implemented method comprising the steps of: reading an attacking source IP address from the attacking data packet (col. 4, lines 43-67, col. 7, lines 10-18, col. 3, lines 61-67, col. 4, lines 1-26, col. 5, lines 5-22, col. 6, lines 19-36); and preventing an incoming data packet comprising the attacking source IP address from entering the host network through the host router (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 10, lines 19-42).

33. As per claim 34-35, Maher discloses the method wherein said preventing step comprises the steps of: determining whether the incoming data packet comprises the attacking source IP address; rejecting the incoming data packet in response to a determination that the incoming data packet comprises the attacking source IP address;

and accepting the incoming data packet in response to a determination that the incoming data packet does not comprise the attacking source IP address, and comprising the step of writing the attacking source IP address to an access control list of the host router, the access control list identifying a source from which the host router will reject a data packet, wherein said determining step comprises determining whether the access control list comprises the source IP address of the incoming data packet (col. 3, lines 61-67, col. 4, lines 1-26, col. 5, lines 5-22, col. 6, lines 19-36).

34. As per claim 36, Maher discloses the method comprising the step of storing the attacking source IP address in an access control file (col. 3, lines 61-67, col. 4, lines 1-26, col. 5, lines 5-22, col. 6, lines 19-36), wherein said writing step comprises writing the contents of the access control file to the access control list of the host router (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 10, lines 19-42).

35. As per claim 37, Maher discloses the method comprising the steps of: detecting a revised version of the access control file; and updating the access control list of the host router to correspond to the revised access control file in response to detecting the revised access control file (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 10, lines 19-42, col. 3, lines 61-67, col. 4, lines 1-26, col. 5, lines 5-22, col. 6, lines 19-36).

36. As per claim 38, Maher discloses The method according to claim 35, further comprising the step of applying the access control list to an incoming interface of the host router (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 10, lines 19-42).

37. As per claim 39-40, Maher discloses the method comprising the steps of: storing a block time for the attacking source IP address, the block time indicating a time period during which said preventing step is performed; determining whether the block time has expired; and discontinuing said preventing step in response to a determination that the block time has expired, and comprising the steps of: storing a block time for the attacking source IP address, the block time indicating a time period during which said preventing step is performed; determining whether the block time has expired; and removing the attacking source IP address from the access control list of the host router in response to a determination that the block time has expired (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 10, lines 19-42, col. 3, lines 61-67, col. 4, lines 1-26, col. 5, lines 5-22, col. 6, lines 19-36).

38. As per claim 42, and 51 Maher discloses a computer-implemented method comprising the steps of: reading an attack target IP address from one of the plurality of attacking data packets; and preventing an incoming data packet having the attack target IP address from entering the host network through the host router (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 10, lines 19-42, col. 3, lines 61-67, col. 4, lines 1-26, col. 5, lines 5-22, col. 6, lines 19-36).

39. As per claim 43-44, Maher discloses the method wherein said preventing step comprises the step of sending the incoming data packet having the attack target IP address to a null interface of the host router, and determining whether the incoming data packet comprises the attack target IP address; accepting the incoming data packet in response to a determination that the incoming data packet does not comprise the

attack target IP address; and sending the incoming data packet to a null interface of the host router in response to a determination that the incoming data packet comprises the attack target IP address (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 10, lines 19-42, col. 3, lines 61-67, col. 4, lines 1-26, col. 5, lines 5-22, col. 6, lines 19-36).

40. As per claim 45, Maher discloses the method comprising the step of automatically updating an upstream router coupled to the host router to direct a data packet destined for the attack target IP address to a null interface of the upstream router (col. 3, lines 61-67, col. 4, lines 1-26, col. 5, lines 5-22, col. 6, lines 19-36, col. 6, lines 58-67, col. 7, lines 1-9).

41. As per claim 46-48, Maher discloses the method comprising the step of writing the target IP address to a null route list of the host router, the null route list identifying a target IP address for which a data packet will be sent to the null interface of the host router, wherein said determining step comprises the step of comparing the target IP address of the incoming data packet to the null route list to determine whether the incoming data packet comprises the attack target IP address, comprising the step of storing the attacking source IP address in a null route file, wherein said writing step comprises writing the contents of the null route file to the null route list of the host router, and comprising the steps of: detecting a revised version of the null route file; and updating the null route list of the host router to correspond to the revised null route file in response to detecting the revised null route file (col. 1, lines 45-67, col. 2, lines 1-5, col.

5, lines 44-58, col. 6, lines 19-36, col. 10, lines 19-42, col. 3, lines 61-67, col. 4, lines 1-26, col. 5, lines 5-22, col. 6, lines 19-36).

42. As per claim 49, Maher discloses the method comprising the steps of: storing a block time for the attack target IP address, the block time indicating a time period during which said preventing step is performed; determining whether the block time has expired; and discontinuing said preventing step in response to a determination that the block time has expired (col. 4, lines 43-67, col. 7, lines 10-18, col. 3, lines 60-67, col. 4, lines 1-26, col. 6, lines 19-36).

43. As per claim 50, Maher discloses the method comprising the steps of: storing a block time for the attack target IP address, the block time indicating a time period during which said preventing step is performed; determining whether the block time has expired; and removing the attack target IP address from the null route list of the host router in response to a determination that the block time has expired (col. 4, lines 43-67, col. 7, lines 10-18, col. 3, lines 60-67, col. 4, lines 1-26, col. 6, lines 19-36, col. 3, lines 61-67, col. 4, lines 1-26, col. 5, lines 5-22, col. 6, lines 19-36).

44. As per claim 52, Maher discloses a system comprising: an interface, coupled to the host router, operable for communicating data packets to and from the host router (col. 4, lines 43-67, col. 7, lines 10-18); a database operable for storing a signature for an attack type of the attack, the attack type comprising a plurality of data packets; a packet sniffing module operable for collecting a data packet from data received by the host router, the data packet comprising information indicating the attack; and a decision module operable for detecting the attack by determining whether the information in the

data packet matches the signature stored in the database (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 10, lines 19-42).

45. As per claim 53, Maher discloses the system wherein said countermeasure module is further operable for providing a pathway for an offensive countermeasure against a source of the attack (col. 3, lines 60-67, col. 4, lines 1-26, col. 6, lines 19-36).

46. As per claim 54, Maher discloses the system comprising a self-learning module operable for generating the signature by identifying a repetitive pattern in the plurality of data packets of the attack type (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 8, lines 27-64, col. 10, lines 19-42).

47. As per claim 55, Maher discloses the system wherein the information in the data packet comprises information from a header of the data packet (col. 4, lines 43-67, col. 5, lines 58-67).

48. As per claim 56-57, Maher discloses the system wherein the signature comprises a repetitive pattern of information in the plurality of data packets of the attack type, wherein the repetitive pattern comprises information included in a header of each data packet of the attack type (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 8, lines 27-64, col. 10, lines 19-42).

49. As per claim 58, Maher discloses the system wherein said decision module is further operable for confirming the attack before said countermeasure module initiates the defensive countermeasure (col. 3, lines 60-67, col. 4, lines 1-26, col. 6, lines 19-36).

50. As per claim 59, Maher discloses the system wherein said decision module is operable for confirming the attack by determining whether a current network load

exceeds a specified load threshold, and wherein the decision module confirms the attack in response to a determination that the current network load exceeds the specified load threshold (col. 4, lines 43-67, col. 7, lines 10-18, col. 3, lines 60-67, col. 4, lines 1-26, col. 6, lines 19-36).

51. As per claim 60, Maher discloses the system comprising a countermeasure module operable for initiating a defensive countermeasure to protect the host network from the attack in response to the decision module detecting the attack (col. 3, lines 60-67, col. 4, lines 1-26, col. 6, lines 19-36).

52. As per claim 61-62, Maher discloses the system comprising a trace route module operable for tracing a route of the attack to determine whether a single source produced the attack, wherein said countermeasure module is further operable for initiating a single-source, defensive countermeasure in response to a determination that a single source produced the attack and for initiating a multiple-source, defensive countermeasure in response to a determination that a single source did not produce the attack, and comprising a router daemon module operable for automatically running said trace route module for tracing the route and said countermeasure module for initiating the defensive countermeasure (col. 3, lines 60-67, col. 4, lines 1-26, col. 6, lines 19-36, col. 3, lines 61-67, col. 4, lines 1-26, col. 5, lines 5-22, col. 6, lines 19-36).

53. As per claim 63, Maher discloses the system wherein said packet sniffing module is further operable for collecting a plurality of data packets from data received by the host router, and wherein said trace route module is further operable for determining that a single source produced the attack by determining whether a source IP address in

each data packet is the same (col. 4, lines 43-67, col. 7, lines 10-18, col. 3, lines 61-67, col. 4, lines 1-26, col. 5, lines 5-22, col. 6, lines 19-36).

54. As per claim 64, Maher discloses a system comprising: an interface, coupled to the host router, operable for communicating data packets to and from the host router (col. 4, lines 43-67, col. 7, lines 10-18); a packet sniffing module operable for collecting a plurality of data packets from data received by the host router; and a decision module operable for detecting the attack by comparing information in respective data packets to determine if any pair of data packets comprise similar information (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 10, lines 19-42).

55. As per claim 65, Maher discloses the system comprising a countermeasure module operable for initiating a defensive countermeasure to protect the host network from the attack in response to detection of the attack (col. 3, lines 60-67, col. 4, lines 1-26, col. 6, lines 19-36).

56. As per claim 66, Maher discloses the system wherein the information in the respective data packets comprises information of a header in the respective data packets (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 8, lines 27-64, col. 10, lines 19-42).

57. As per claim 67, Maher discloses the system wherein said decision module is further operable for confirming the attack by determining whether a current network load exceeds a specified load threshold, and wherein the decision module confirms the attack in response to a determination that the current network load exceeds the

specified load threshold (col. 4, lines 43-67, col. 7, lines 10-18, col. 3, lines 60-67, col. 4, lines 1-26, col. 6, lines 19-36).

58. As per claim 68, Maher discloses the system comprising a self-learning module operable for determining whether the attack comprises a new attack type and for learning a new signature of the new attack type in response to a determination that the attack comprises a new attack type (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 10, lines 19-42, col. 6, lines 58-67, col. 7, lines 1-9).

59. As per claim 69, Maher discloses the system comprising a database, wherein said learning module is further operable for identifying a repetitive pattern in data from the plurality of data packets of the attack and for storing the repetitive pattern in the database as the new signature of the new attack type (col. 1, lines 45-67, col. 2, lines 1-5, col. 5, lines 44-58, col. 6, lines 19-36, col. 8, lines 27-64, col. 10, lines 19-42).

60. As per claim 70, Maher discloses the system wherein the data from the plurality of data packets comprises information in a header of each respective data packet (col. 4, lines 43-67, col. 5, lines 58-67).

Conclusion

61. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mohammad w. Reza whose telephone number is 571-272-6590. The examiner can normally be reached on M-F (9:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, MOAZZAMI NASSER G can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mohammad Wasim Reza

AU 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

9/21/06